

1 / 5

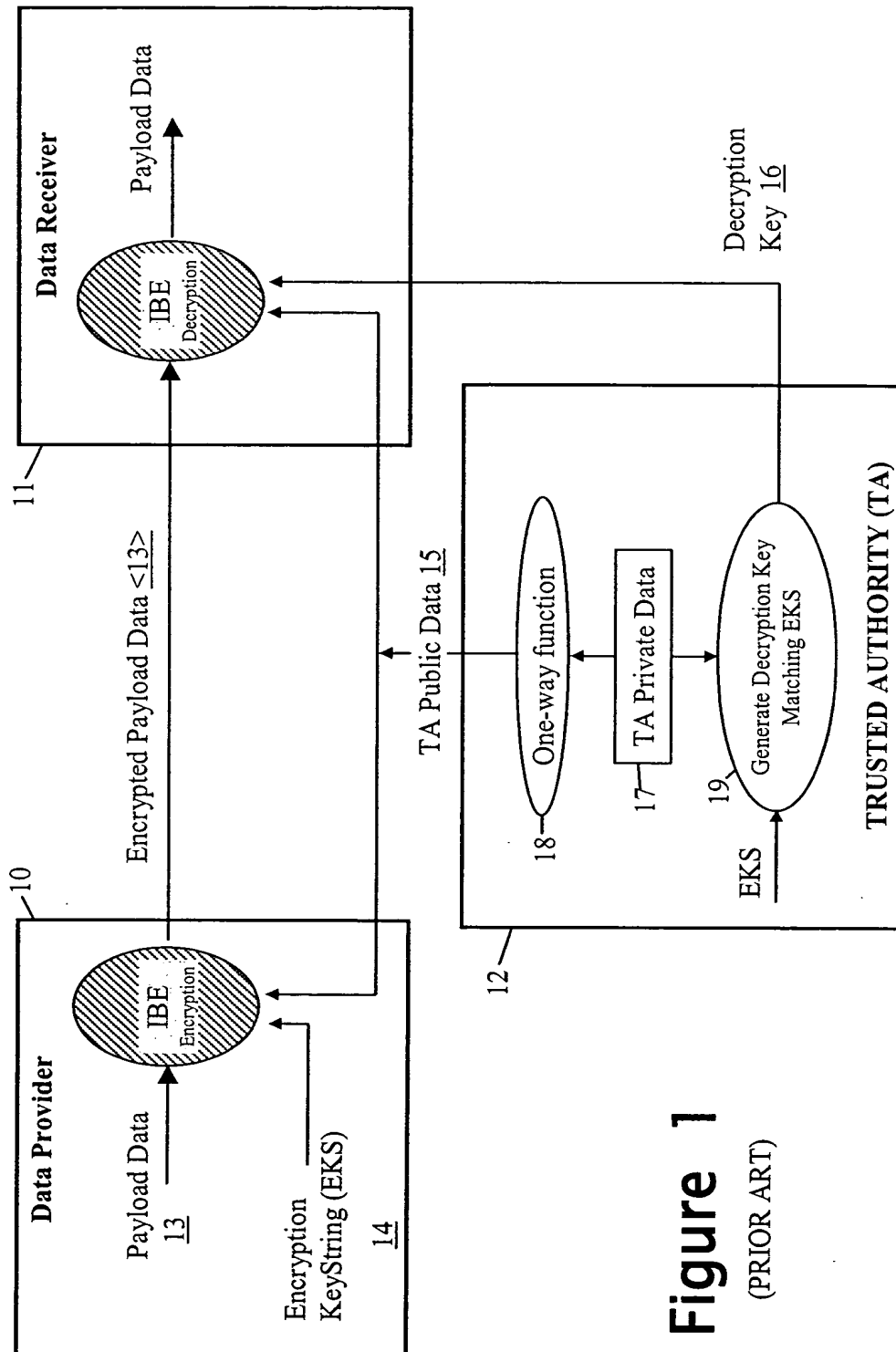
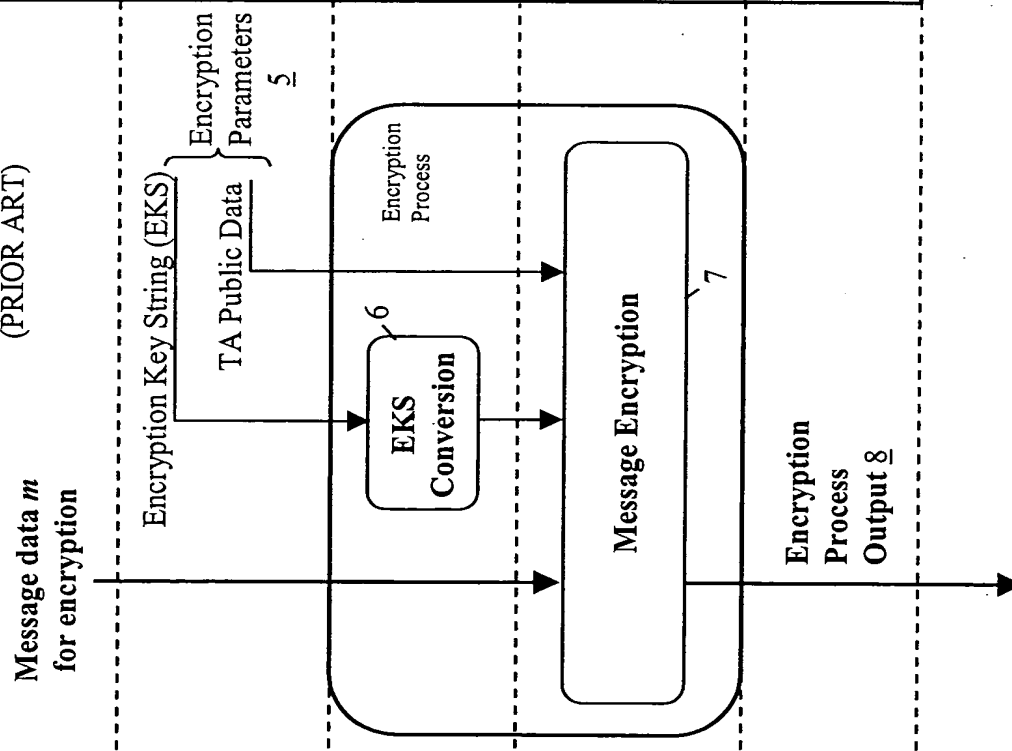
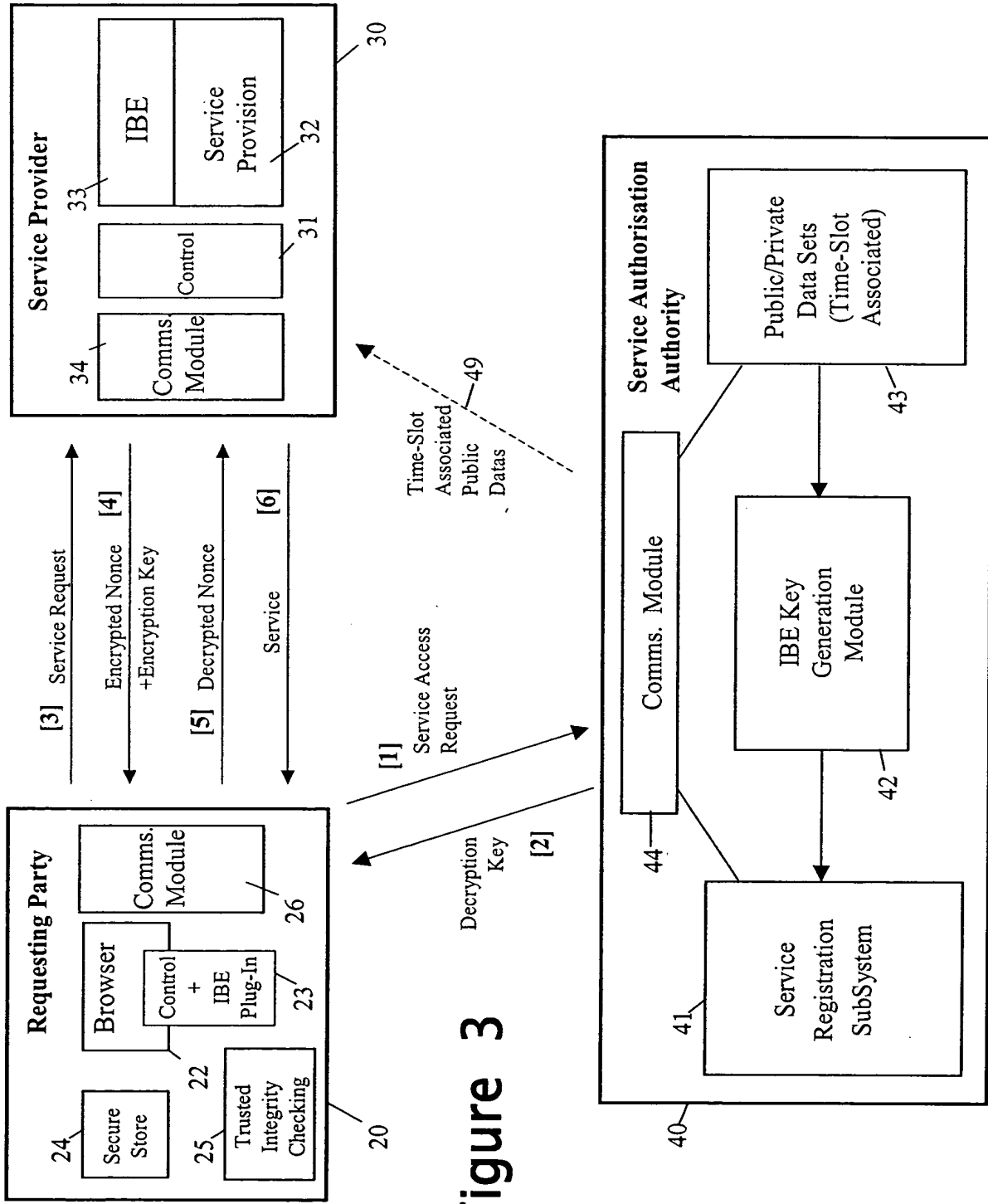


Figure 2
(PRIOR ART)



Identifier-Based Method		
Quadratic Residuosity	Bilinear Mappings $p: G_1 \times G_1 \longrightarrow G_2$	RSA Based
EKS Modulus N	EKS (P, sP) where P is in G_1 s is secret of TA	EKS Modulus n
$K = \#(\text{EKS})$	“Map-to-point” hash $Q_{\text{ID}} = H_f(\text{EKS})$ where $H_f: \{0,1\}^* \longrightarrow G_1$	$e = \#(\text{EKS}) \bmod n$
For each bit: $s_+ \equiv (t_+ + K/t_+) \bmod N$ $s_- \equiv (t_- - K/t_-) \bmod N$	$V = m \oplus H_2(t(sP, rQ_{\text{ID}}))$ where: $H_2: G_2 \longrightarrow \{0,1\}^*$ r is a random number	$m^e \bmod n$
For each bit: s_+, s_- (knowledge of EKS and TA concerned also needs to be available)	$V, U (= rP)$	$m^e \bmod n$



4/5

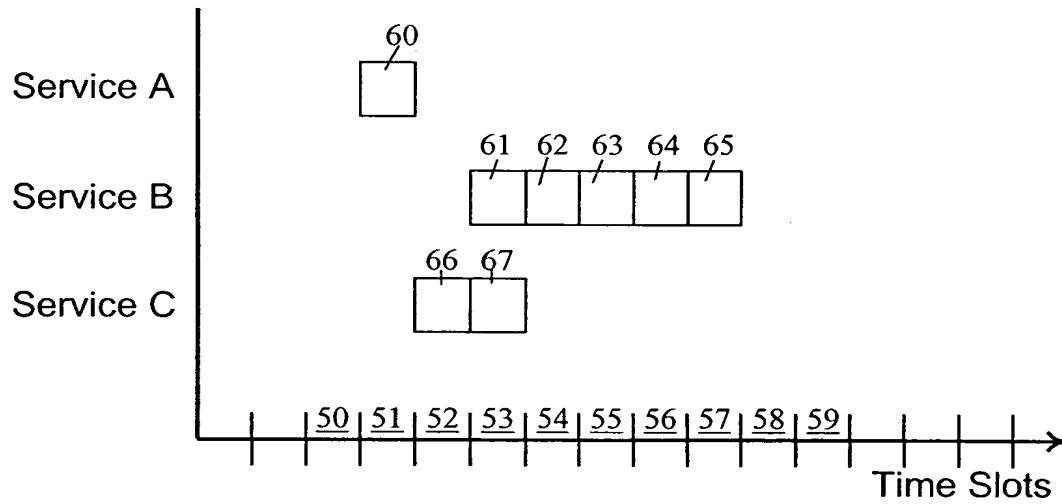


Figure 4

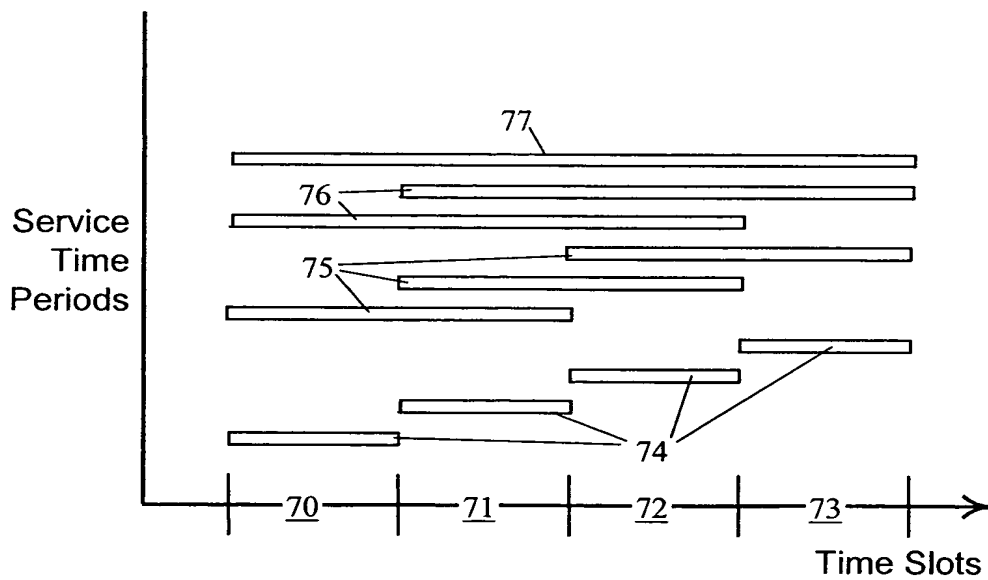


Figure 5

5 / 5

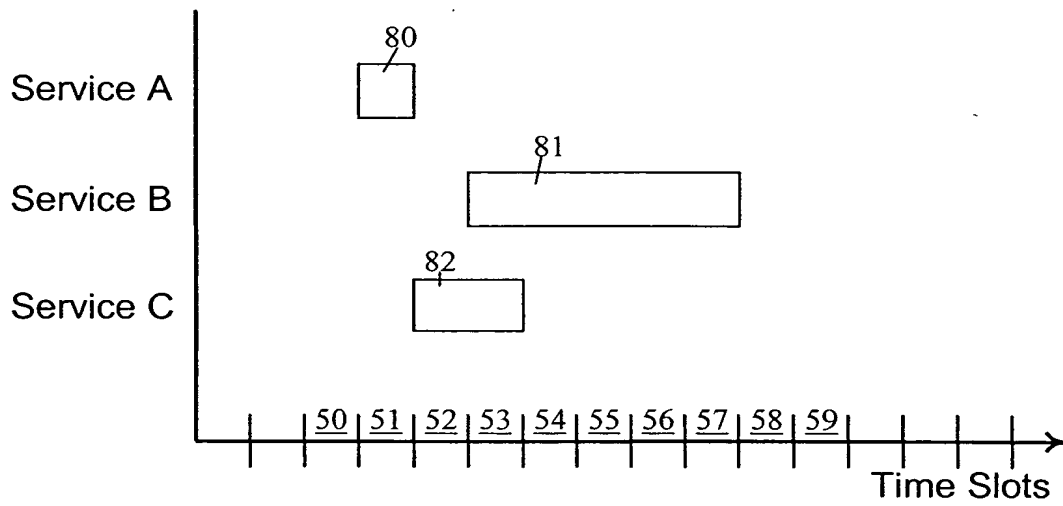


Figure 6